The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:
4/13/2010

SUBJECT:
Vulnerabilities in Microsoft Visio Could Allow Remote Code Execution (MS10-028)

OVERVIEW:
Two new vulnerabilities have been discovered in Microsoft Visio, a program used for creating flowcharts and diagrams. These vulnerabilities can be exploited by opening a specially crafted Visio file (.VSD) received as an email attachment, or by visiting a website and opening a specially crafted Visio file. Successful exploitation could allow an attacker to gain the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

SYSTEMS AFFECTED:

Microsoft Visio 2002
Microsoft Visio 2003
Microsoft Visio 2007

RISK:

Government:
Large and medium government entities: **High**
Small government entities: **High**

Businesses:
Large and medium business entities: **High**
Small business entities: **High**

Home users: Low – due to our assumption that Visio is not widely utilized by the average home user

DESCRIPTION:
Two new vulnerabilities have been identified in Microsoft Visio that could allow remote code execution. These remote code execution vulnerabilities are due to the way that Microsoft Visio validates attributes or calculates indexes when handling a specially crafted Visio file (.VSD). These vulnerabilities can be exploited via an email attachment or through the Web. In the email based scenario, the user would have to open the specially crafted Visio file as an email attachment. In the Web based scenario, a user would visit a website and then open the specially crafted Visio file that is hosted on the page.

Successful exploitation could allow an attacker to gain the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

RECOMMENDATIONS:
The following actions should be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.

- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to open e-mail attachments from unknown users or suspicious e-mails from trusted sources.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by attachments and hypertext links contained in emails especially from un-trusted sources.

REFERENCES:

Microsoft:
http://www.microsoft.com/technet/security/bulletin/ms10-028.mspx

CVE:
http://secunia.com/advisories/cve_reference/CVE-2010-0254
http://secunia.com/advisories/cve_reference/CVE-2010-0256

Security Focus:
http://www.securityfocus.com/bid/39300
http://www.securityfocus.com/bid/39302